more security. usd

HACKER CONTEST

Anmeldeaufgabe

Sommersemester 2025

usd HeroLab

Autor	**Matthias Göhring, Tobias Hamann, Tim Wörner**
Datum	**31.03.2025**
Klassifizierung	Öffentlich (V0)

1 Allgemeines

Für die Teilnahme am Hacker Contest steht leider nur eine begrenzte Anzahl Plätze zur Verfügung. Zum Zwecke der Auswahl wird die folgende Anmeldeaufgabe gestellt. Anhand der abgegebenen Lösung wird über die Teilnahme entschieden.

Die Aufgabe wird in Form eines Docker Containers bereitgestellt und kann unter folgendem Link mit folgendem Passwort heruntergeladen werden:

https://transfer.usd.de/index.php/s/jaL3GCam8nSWAaT
Passwort: **G00dLuck&H4ppyHacking:)**

Bei der Bearbeitung der Challenge dürfen beliebige Tools zur Unterstützung eingesetzt werden. Es bietet sich an, eine virtuelle Maschine mit einer Linux Distribution einzusetzen, die für Hackingtools spezialisiert ist (beispielsweise Kali Linux oder ParrotOS). Auf diesen Distributionen sind viele für die Challenge nützliche Tools bereits vorinstalliert.

2 Aufgabe

Die Aufgabe ist es, den bereitgestellten Docker Container auf Schwachstellen zu untersuchen.

Der Container kann mit dem folgenden Befehl gebaut werden:
```
docker build -t hcss25
```
Anschließend wird er gestartet:
```
docker run --rm --privileged -v /sys/fs/cgroup:/sys/fs/cgroup:rw --
cgroupns=host -p 1337:1337 --name hcss25 hcss25
```
Die Webapp ist auf localhost:1337 verfügbar.

2.1 Szenario

Ein guter Freund hat dich gebeten, seine selbstgeschriebene Website auf Schwachstellen zu untersuchen. Diese stellt er dir als Docker Container bereit. Nach deiner Abnahme möchte er den Container auf einem Linux Server mit öffentlicher IP installieren.

Wie sich herausstellt, ist es für Angreifer möglich, „root“-Zugriff innerhalb des Containers zu erhalten. Dabei werden drei Schwachstellen nacheinander ausgenutzt.

Die Aufgabe besteht darin, die Schwachstellen zu identifizieren und in eine sinnvolle Angriffskette zu bringen. In der Abgabe soll die Vorgehensweise eines möglichen Angreifers detailliert beschrieben und wenn möglich Skripte zum Ausnutzen der einzelnen Schwachstellen bereitgestellt werden.

Es wird davon ausgegangen, dass ein Angreifer vollständiges Wissen über die interne Funktionsweise des Docker Containers hat (keine „Security through obscurity“). Insbesondere darf (bzw. muss) der Quelltext der Website verwendet werden um Schwachstellen zu identifizieren. Es wird jedoch im Idealfall davon ausgegangen, dass Passwörter aus dem Code für den Angreifer unbekannt sind. Die Präsenz von Passwörtern stellt somit keine Schwachstelle dar.

Auch Teile einer Angriffskette können abgegeben werden und werden mit Teilpunkten bewertet. Es ist jedoch nicht notwendig ein Passwort zu kennen, um „root“-Zugriff zu bekommen. Eine Abgabe, die Passwörter aus dem Code verwendet, kann somit in der Bewertung nicht die volle Punktzahl erhalten.

2.2 Bearbeitungszeitraum

Der Bearbeitungszeitraum beginnt mit der Veröffentlichung der Aufgabe. Er endet am **21.04.25 um 23:59 Uhr**. Alle Abgaben, die nach dieser Frist erfolgen, können leider nicht berücksichtigt werden.

2.3 Abgabemodalitäten

Abgaben werden ausschließlich über die folgende URL entgegengenommen:

https://transfer.usd.de/index.php/s/H8QWYrizS8MKLTH
Passwort (notwendig für den Upload): **G00dLuck&H4ppyHacking:)**
Dateiname: **HC-SoSe25_(TU/HDA)_<Vorname>.<Nachname>.pdf**

Als Abgabe wird ein Bericht mit allen Informationen im **PDF-Format** erwartet. Der vollständige Name, die Matrikelnummer und die (Universitäts-)E-Mail-Adresse müssen **auf der ersten Seite** des PDF-Dokuments vermerkt sein. Die Form fließt in die Bewertung mit ein! Gruppenarbeit oder Gruppenabgaben sind nicht gestattet. Plagiate führen zum Ausschluss aller Beteiligten von der Teilnahme am Hacker Contest.

Aus dem Bericht sollen Details zur Vorgehensweise und Ausnutzung von Schwachstellen, sowie verwendete Tools hervorgehen.

Fragen zur Aufgabenstellung bitte per E-Mail an hackercontest@usd.de.